SIENNA: Insider Resistant Context-Based Pairing for Multimodality Sleep Apnea Test

Samson Aggelopoulos
Marionne Casipit
Brian Lu
Stephanie Aelmore
Willy Chang
Alana Power

Professor Yao Zheng

Introduction

- Obstructive sleep apnea (OSA)
  - Over 25 million sufferers
  - Traditional testing is obtrusive and expensive
- In-Lab Polysomnography (PSG)
  - Requires patient to be in-lab overnight
  - Multiple instruments of sensors and electrodes
  - Testing facilities are scarce
- At-Home OSA Screenings
  - Convenient and cost-effective
  - Vulnerable to test fraud

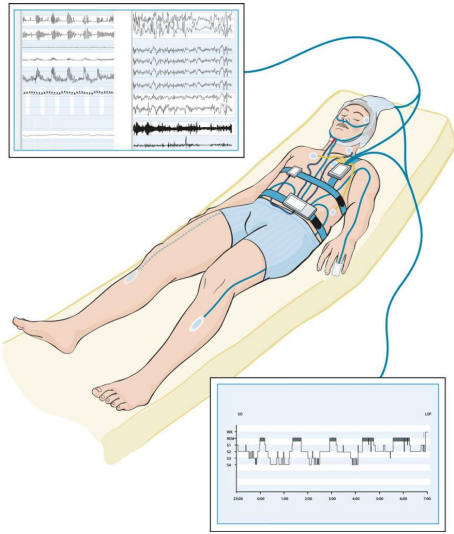

Fig 2-1.

At-Home OSA Screening Modalities

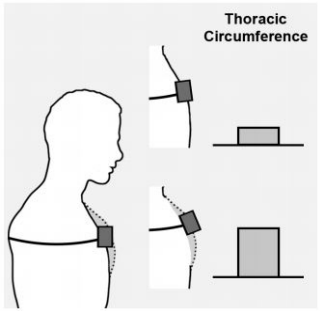

Fig 3-1.

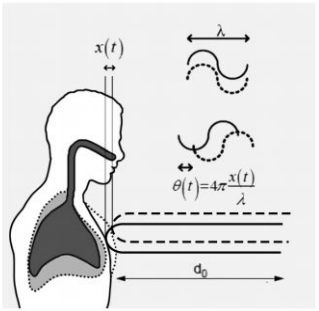

Fig 3-2.

- Respiratory belt
  - Measure changes in thoracic circumference from respiration
- Physiological radar monitoring system (PRMS)
  - Measure phase shift of reflected signals from the patient's chest movements
- Mobile OSA app
  - Aggregate OSA screening data from sensing modalities

Problem Description

- Pairing Vulnerability
  - Belt paired with the user's phone by a medical technician
  - PRMS paired without supervision at the user's home
  - Non-compliant user may exploit the unsupervised pairing process
- Design goals
  - Pair two devices with zero human interaction
  - Secure the pairing process against a co-located adversary
- Adversary Models
  - Eavesdropper: Extract security context, decrypt and review data
  - Spoof: Transmit false data, manipulate OSA test outcome

in**SI**der r**E**sista**N**t co**N**text-based p**A**iring (**SIENNA**)

- JADE-ICA – Algorithm for separating independent sources from a mixed signal
- Level-crossing quantization – Produces a binary key from the breathing pattern
- Fuzzy Commitment – Scheme for validating biometric information
- Friendly Jamming – System for partially jamming a signal to resist eavesdropping

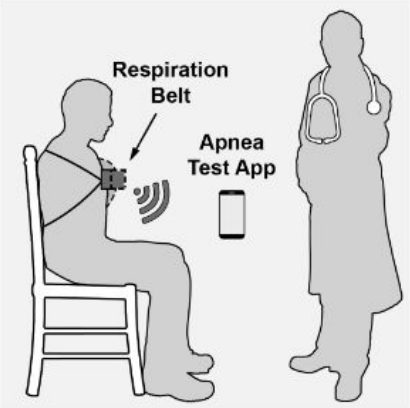

Fig. 5-1

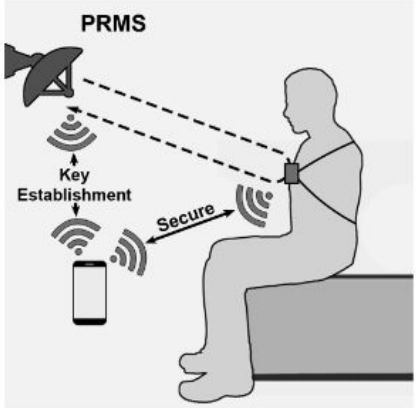

Fig. 5-2

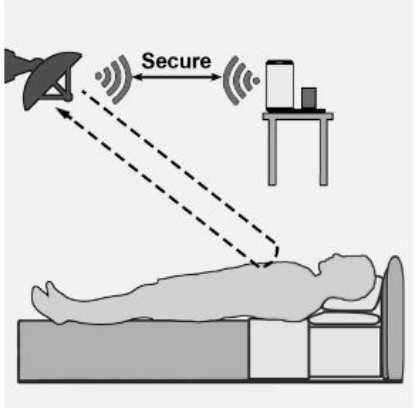

Fig. 5-3

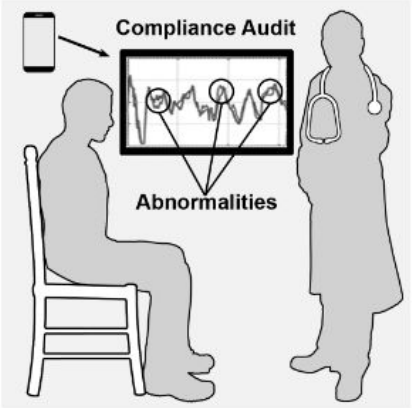

Fig. 5-4

Methodology

- Breathing Separation
  - JADE-ICA
    - Input signals in the form of a matrix are “whitened” using PCA to produce orthogonal columns
    - Whitened matrix is rotated to produce independent rows
- Fingerprinting
  - Level-crossing quantization
    - Quantizer QTZ(x) produces a distinct binary code based on where the signal falls between levels

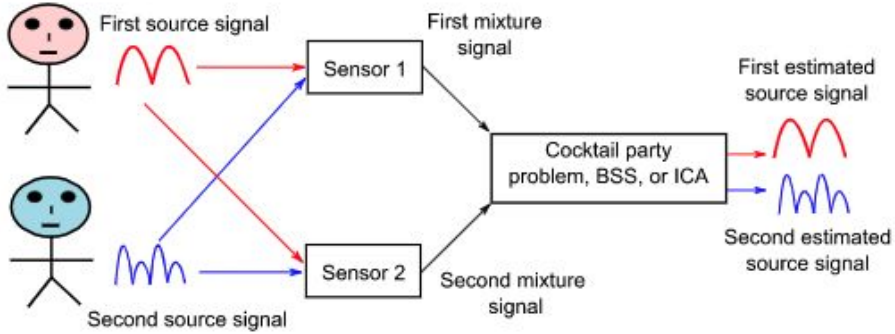

Fig. 6-1: Illustration of mixed source signals separated with ICA

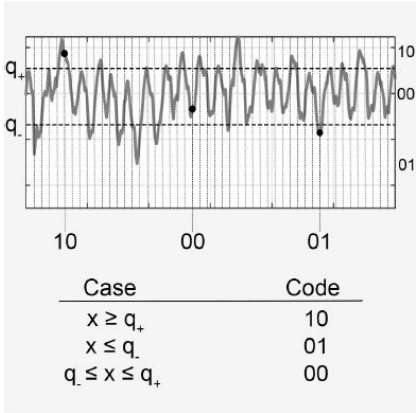

Fig. 6-2: Illustration of Level-crossing quantization with two bits.

Methodology cont.

- Context-Based Device Pairing
  - Fuzzy Commitment
    - Secret value σ (v bits), Hash function H (μ bits), Opening feature φ, Commitment χ
    - σ can be revealed if and only if the Hamming Distance is within threshold τ
    - Concealing if σ cannot be guessed with p>1/2^v
    - Binding if incorrect feature rejected with p>1/2^μ
    - v = 128, and μ = 256 ⟶ similar to SHA-256
- Insider Resistant
  - Dialog-Code-Based Friendly Jamming
    - Transmitter duplicates each symbol, and receiver jams a random selection
    - Eavesdropper won't know which ones are jammed

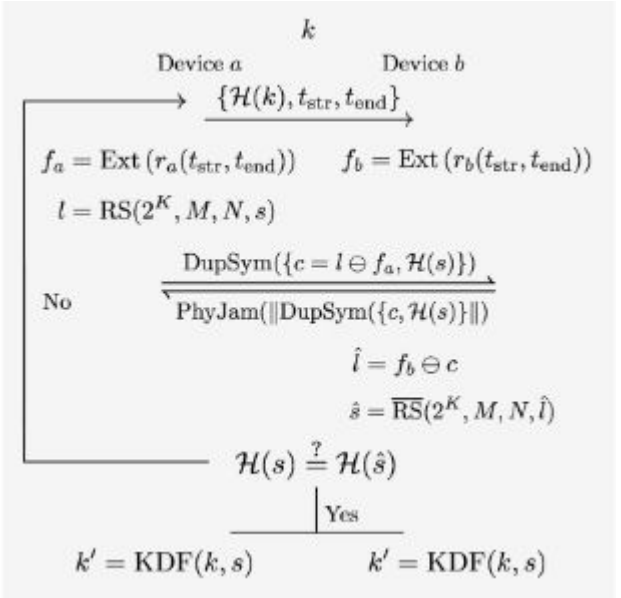

Fig. 7-1: Overview of the Insider Resistant Device Pairing process.

Implementation and Materials

Sienna was developed and tested using:

- PRMS
  - TMYTEK mmWave Kit, NI USRP
- Wireless Respiratory belt
  - Pneumotrace 1132
- OSA app
  - Android app with modality switching
- Eavesdropper
  - BLE with Kismet and Ubertooth

Experiment Setup

- Initial data collection done outdoors with beach mats, and indoors with beds
- Experiments ran for hour long intervals
- Eavesdropping and spoofing attacks were attempted in intervals
- The data was analyzed and verified offline

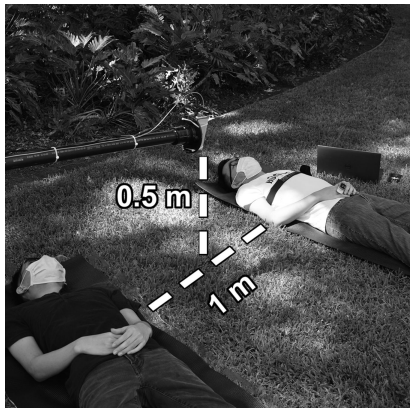

Fig 9-1.

Fig 9-2.

Fig 9-3.

Fig 9-4.

Results and Analysis

- Performance of fingerprint extraction
  - Breathing signature quantized in parallel
  - Quantization step size to 0.05cm @10samples/sec
- Quality of binary fingerprint
  - Hamming distance between fingerprints
  - SIENNA can be set to 70% for optimal performance
- Performance of key evolution
  - Measured randomness of fuzzy commitment
  - Entropy drops due to redundancy of motions
- Performance under adversarial settings
  - BER@receiver vs. aggregated BER@attacker
  - Jamming signal can suppress approximately 50%

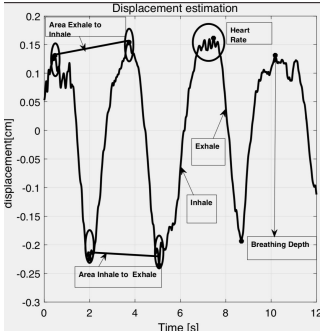

Fig 10-1. Reconstructed signal after QTZ

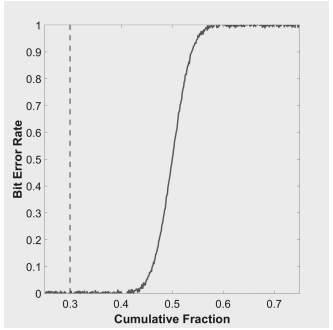

Fig 10-2. BER of jammed signal

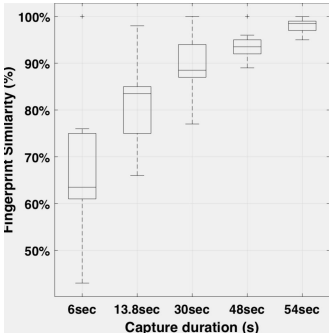

Fig 10-3. Similarity of same subject

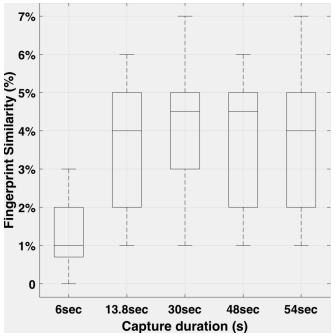

Fig 10-4. Similarity of different subject

Conclusion

- SIENNA: insider-resistant context-based pairing
  - Employs fuzzy commitment, friendly jamming, JADE-ICA
  - Leverages unique breathing patterns for secure pairing
- Security Analysis and Evaluation
  - Attacker w/out knowledge: is mitigated through fuzzy commitment
  - Attacker w/ general knowledge: is mitigated by increasing entropy
  - Attacker w/ perfect knowledge: is mitigated by friendly jamming
  - Accumulated BER of fuzzy commitment with friendly jamming is well beyond decodable for an attacker
- Publications
  - “Insider-Resistant Context-Based Pairing for Multimodality Sleep Apnea Test” submitted to Globecom 2021
  - Technical Report available at https://arxiv.org/abs/2105.00314

Acknowledgements

Special thanks to Dr. Yao Zheng, Dr. Ming Li, Dr. Olga & Victor Lubecke, and Yanjun Pan for mentoring this project.

Great thanks to TMYTEK for their support and equipment.

This work is partly supported by NSF grants and ARO grant

- Dr. Yao Zheng: CNS-1948568
- Dr. Ming Li: W911NF-19-1-0050
- Dr. Olga & Victor Lubecke: IIP-1831303, IIS-1915738

Thank You